To: "Schwartz, Alan" <arsdc@yahoo.com>
To: Michael Bayer <mbayer@erols.com>
Subject: First draft of introductory narrative. RED-NUF report
Fcc: DSB

This is somewhat free-form, but I thought it would be needed, and here's a start.

Sun Dec 2 19:55:31 EST 2001

This study was mounted to assist decision makers with the daunting task of achieving perspective on US vulnerabilities to terrorist attack. When intelligence is available, aggressive preemption and defensive preparation can be and have been of the most effect. Intelligence is often not available, or may be vague or confusing or otherwise subject to misinterpretation. Then its cogency can be enhanced by joining it with a RED Team perspective, what are the most vulnerable/lucrative targets that RED might perceive, or which would render the most harm to BLUE.

Likely, thousands of scenarios have been proposed as suits the station, temperament or experience of the author, or may be plucked as variants of the news headlines. As a matter of common sense, we invest in stringent security for nuclear reactors or munitions dumps, not waiting for explicit inteliigence of a malefactor's plans. History reinforces our concerns to protect the personal safety of the highest levels of government. Now that the ambitions of terrorists have risen, and technology for destruction along with them, there is substantial unanimity that our anticipatory effort be comparable to the tacit threat, that we build our defenses to higher levels before the events.

Scenarios provide useful sensitization, but how to choose which ones for undergirding further investment? Rational choice would entail first hearing them all, putting them in competition for our attention. "All" promptly generates its own problems, especially when fired by infernal ingenuity.

We sought then to begin to design a methodology that would be more manageable than intuitively derived lists, no matter how well inspired. The product will not be one more list, but rather a means of generating lists at whatever level of detail is appropriate, and likewise focussed on the parameters that current intelligence or personal insight would bring to bear.

We started by collecting a diverse group of consultants -- table 1, will indicate the breadth of their disciplinary and occupational backgrounds. And we did collect lists, also informed by known history of terrorist events.

That experience helped us decide how to construct an event space, and to choose for its orthogonal dimensions (or vectors):

BLUE assets -- what we seek to protect
RED weaponry -- to the limits of our imagination
RED delivery systems -- including cooption of our own vehicles or pipelines
Scale of attack -- from [0 = hoax] to, say, 4 [a Hiroshima]

We could then explore each of these vectors systematically, with some assurance of coherence and completeness. Our task was simplified by the work of others, e.g. the US Census Bureau classification of industry (which embraced almost every site our imaginations had proffered.) We saved our own labor and embarassment by relying on others' work on infrastructure and on cybersecurity. We played cultural anthropology and sociology in indexing intangible parts of our social capital -- all that could benefit from more work, though we had the great benefit of a psychiatrist on our team.

This BLUE assets vector is all but ready for critical assessment and enhancement by other specialty groups. One of our recommendations is that we mobilize industry associations across the board to conduct their own studies of criticality and vulnerability. Chemical manufacturing and Financial Services among others were already represented on our team.

Without going to the detail of particular attack scenarios, one of our prescriptions is to concentrate on the BLUE assets; when a critical one is identified one can often discover a potential mode of attack. Then think of the secondary consequences of physical knockout or functional disablement, by whatever weapon (be it HE or BW). Because of these ramifications, infrastructure by definition looms large. Then we also fold in special vulnerabilities (toxic or energy density).

The RED weaponry and delivery systems look straightforward; we have to remind ourselves that standoff weapons (from the planners' perspective) now include suicidal bomb-carriers, but they also include mortar ordnance, grenade launchers, and sniper weapons of substantial range. We did not detail the range of specific biological and chemical weapons potentially at RED's disposal: the most important point is that anthrax is the most efficient targettable microbe we know; but there is a long list of agents ultimately waiting in the wings.

The fourth axis, SCALE, is important to remember -- it is, when the weapon allows, an option at RED's discretion, and thus becomes a proxy for RED intentions. We found we could engage our group indefinitely in spirited discussions on that point -- and decided that there were many RED's, we should not choose one to exclusion of others. Small scale attacks can have large secondary consequences when fueled by public apprehension of invisible toxins, radiation, or germs.

In principle, one could convolute these 4 dimensions, and generate a large space with perhaps 10^6 points; rarely would that be useful, though a random game does help exercise the imagination, and brings out vulnerabilities and consequences that might have been neglected.

Obviously, this looks for automation, and the space becomes a frame for annotation, for special judgments and insights, for recording intelligence, -- a dynamic database whose granularity is under user's control. The annotation would take account of special fragilities or indispensabilities, to remind us of BLUE targets needing special attention. It would also initiate the process of seeking specific I&W, countermeasures, and remediation.

A would-be scenario-writer who has been through this training exercise is more likely to be trustable, that alternative options have been duly considered. Our group did just that, and our own prescripts are in the appendix. Give us a budget of $x billion, and we'll come back with

some kind of allocation, but we need more time to reflect on the work done. Infrastructure will attract the lions' share; but RED and BLUE alike are sure to be influenced by public perceptions of what defines security.